ECONOMICS OF SOFTWARE SECURITY

Traditional View to Security

- Internet is insecure because lack of features
  - Cryptography
  - Authentication
  - Filtering
- Solution: create better technologies
  - Encryption algorithms
  - Security protocols
  - Network security mechanisms

Alternative View

- Applying economic analysis to IT security
- Systems are insecure because people who should fix them have insufficient incentives
- Insecurity is a side effect

Example: Credit Card Fraud

- US banks are liable for costs of card fraud
  - If customer disputes transaction, bank must prove that he is cheating or refund the money
- UK banks often were not
  - They claimed that systems were „secure”
  - Customers carried the burden of proof

Example: Credit Card Fraud (2)

- Staff in UK banks knew that customers will be blamed
- It was OK to be careless
- UK banks ended up suffering massive amounts of fraud
- End result: UK banks spent more money on security, but suffered more fraud
  - US banks spent the money smarter

More on Incentives

- People evaluating software are not the ones who will suffer when they fail
  - „Nobody has been fired for buying IBM”
  - Vendor is responsible for ordering the audit
- Viruses
  - Nowadays, viruses do not attack personal computers
  - They *infect* PCs and use them to attack other sites
  - No need to invest in protection

Network Externalities

- Impact on a party that is not directly involved in economic transaction
- If enough houses have silent alarms, breakins go down
  - You have lower risk of theft even if you do not have alarm
- People who invest in fire safety make other people safer too
- Every person who buys cell phone increases value of my cell phone

Network Externalities (2)

- Externalities do not have to be positive
- I can enjoy air pollution even without owning a car

Tragedy of Commons

- All villagers graze sheep on a common pasture
- Villager adds one sheep
- He gets full benefit for additional sheep
- Costs are shared by other villagers
- Other villagers also start adding sheep

Example: Spam

- Costs to spammers are low
- Very low probability of success is acceptable
- Costs are carried by others

Attack vs. Defence

- Defender needs to patch all bugs
- Attacker needs to discover only one

Open vs Closed Source

- Removing one bug does not improve protection
- Attacks are often based on patches
- Removing vulnerability creates attack for people who have not patched
  - Unless vulnerability is likely to be rediscovered
- BSD example
  - Vulnerabilities were correlated (rediscovered)
  - Number of disclosed vulnerabilities declined over time

Incentive and Asymmetric Information

- CIA discovers hole in Windows
- Report and protect 250 million Americans?
- Keep quiet and attack 400 million Europeans and 100 million Japanese?

- If you attack foreigners, you get credit
- If foreigners attack you, nobody finds out

Network Effects

- Many IT product and service markets have network effects
- Metcalfe's law: the value of the network is the square of the number of users
- Real networks: phones, fax, e-mail
- Virtual networks: PC vs. Mac, Java vs. .NET
- Often the output is dominant firm market where winner takes all

Network Effects (2)

- IT product and service markets usually have high fixed costs and low marginal costs
  - First copy of software costs $10M to produce
  - Second copy costs $1
- Competition can drive down prices to marginal cost of production
- Hard to recover capital investment, unless protected by patent, brand, compatibility
- This can also lead to dominant-firm market structures

Network Effects (3)

- Switching from one product or service to another can be expensive
- Example: switching from Windows to Linux means rewriting apps, training staff
- Shapiro-Varian theorem: the net present value of a software company is the total switching costs
- So major effort goes into managing switching costs – once you have $3000 worth of songs on a $300 iPod, you're locked into iPods

IT Economics and Security

- High fixed/low marginal costs, network effects and switching costs all tend to lead to dominant-firm markets with big first-mover advantage
- So time-to-market is critical
- Microsoft philosophy of 'we'll ship it Tuesday and get it right by version 3' is not perverse behaviour by Bill Gates but quite rational
- Whichever company had won in the PC OS business would have done the same

IT Economics and Security (2)

- When building a network monopoly, you must appeal to vendors of complementary products
- That's application software developers in the case of PC versus Apple
- Lack of security in earlier versions of Windows made it easier to develop applications
- So did the choice of security technologies that dump costs on the user (SSL, not SET)
- Once you've a monopoly, lock it all down!

S-curve of Technology Adaption

- Some new technologies do not achieve the critical mass
- SSH and IPSec also provided other internal benefits so organizations could implement them without waiting for others
- Same with fax machines – they could be used for connecting company offices

Market for Lemons

- Study in asymmetric information
- Suppose a town has 100 used cars for sale: 50 good ones worth $2000 and 50 lemons worth $1000
- What is the equilibrium price of used cars?

Market for Lemons

- Study in asymmetric information
- Suppose a town has 100 used cars for sale: 50 good ones worth $2000 and 50 lemons worth $1000
- What is the equilibrium price of used cars?
- If $1500, no good cars will be offered for sale …

Market for Lemons (2)

- Security products are often a ‘lemons market’
- Buyers do not know whether the product really works
- Ineffective products drive the price down

Trust Certifications

- Websites with a TRUSTe certification are more than twice as likely to be malicious
- The top Google ad is about twice as likely as the top free search result to be malicious
- Conclusion: ‘Don’t click on ads’

Types of Users

- Traditional: good users follow rules, bad users break rules
- New type of users: „selfish” or rational users
- Try to take advantage of positive network externalities (freeriding)
  - In P2P sharing systems, download without uploading
  - If everybody else has alarm, don't install one

What Effort is Needed for Protection

- Example: flood defenses in an tropical island
  - Each family responsible for defenses on their land
  - All the island depends on the laziest family
- Example: defence against ICBM
  - Determined by the best shot
- What type of effort is securing a software system?

What Effort is Needed for Protection (2)

- Introducing a bug – weakest programmer
- Developing good security architecture – best architect
- Security testing – sum of efforts

Trusted Computing

- Supposed to assure secure environment for running programs
  - Protects programs against owner of the machine
- Possible effects:
  - Can limit innovation
  - Control transferred to media owner instead of computer owner
  - Money starts moving from record companies to TC vendors (especially Apple)

Security Measures in the Future?

- Content protection
- Protecting price differentiation
- Ensuring lock-in
  - Authenticating toner cartridges, mobile batteries